RANDOM NUMBERS GENERATOR

Patent Number: JP6051957
Publication date: 1994-02-25
Inventor(s): HASHIMOTO TOKUO; others: 01
Applicant(s): RICOH CO LTD
Requested Patent: JP6051957
Application Number: JP19920224702 19920731
Priority Number(s):
IPC Classification: G06F7/58
EC Classification:
Equivalents:

Abstract

PURPOSE:To generate a random numbers string with different arrangement of pulse string by switching the feedback position of a linear feedback shift register(LFSR) after the random numbers string is generated extending over a certain period decided in advance.
CONSTITUTION:The LFSR is comprised of a shift register 401 of seven bits, an exclusive OR circuit 404, and a selector 402 which selects the feedback position. Respective bit data r1-r7 of the shift register 401 are taken out in parallel, and binary random numbers b0-b6 in which a shift-in side is set as an LSB, and a shift-out side as an MSB can be obtained. Furthermore, a two-bit binary counter 403 is connected to the selector 402, and the counter 403 receives contents in sequence of 00 01 10 11 00 corresponding to the input of a count clock 407, and the bit data r1 is selected for 00, and r6 for 01, and r4 for 10, and r3 for 11, then, they are fed back. Therefore, the arrangement of a pulse can be changed by changing the feedback position of the LFSR.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平6－51957

(43)公開日　平成６年(1994)２月25日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　7/58		Ａ　9188－5Ｂ		

審査請求　未請求　請求項の数４(全　７　頁)

(21)出願番号　特願平4－224702

(22)出願日　平成４年(1992)７月31日

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号

(72)発明者　橋本　篤男
東京都大田区中馬込１丁目３番６号　株式会社リコー内

(72)発明者　樽木　杉高
東京都大田区中馬込１丁目３番６号　株式会社リコー内

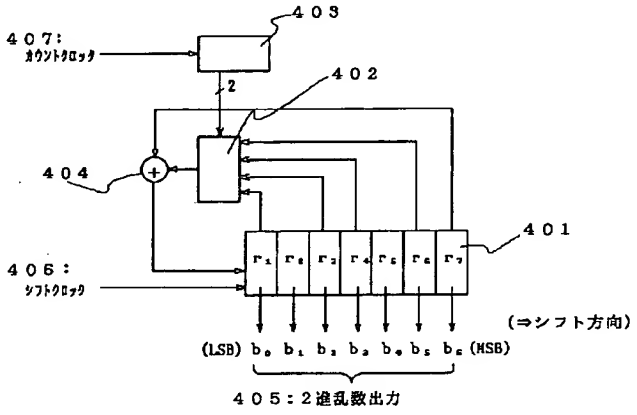
(74)代理人　弁理士　鳥居　洋

(54)【発明の名称】　乱数発生装置

(57)【要約】

【目的】　乱数発生装置に関し、パルス列の並びが異なる乱数列を発生することができる乱数発生装置を提供することを目的とする。

【構成】　ｎ次の最大周期列信号を生成するＬＦＳＲを備えた乱数発生装置において、あらかじめ定められた期間にわたって乱数列を発生した後、カウンタ４０３と、カウンタ４０３の内容に対応して前記ＬＦＳＲのシフトレジスタ５０１のフィードバック位置を切り替えるセレクタ５０２からなり、予め定められた期間にわたって乱数列を発生した後、前記ＬＦＳＲのフィードバック位置を切り替える手段を設ける構成とする。



1

【特許請求の範囲】

【請求項１】　ｎ次の最大周期列信号を生成する第一のリニアフィードバックシフトレジスタ（以後、リニアフィードバックシフトレジスタをＬＦＳＲと略記する。）を備えた乱数発生装置において、あらかじめ定められた期間にわたって乱数列を発生した後、前記ＬＦＳＲのフィードバック位置を切り替える手段を設けたことを特徴とする乱数発生装置。

【請求項２】　上記手段が、カウンタと、カウンタの内容に応じてＬＦＳＲのフィードバック位置を切り換えるセレクタとを備えることを特徴とする請求項１に記載の乱数発生装置。

【請求項３】　上記手段が、ｍビットのシフトレジスタと、該シフトレジスタに格納されたビットデータに従って前記ＬＦＳＲのフィードバック位置を切り換えるセレクタとを備えることを特徴とする請求項１に記載の乱数発生装置。

【請求項４】　上記手段が、最大周期列信号を生成する第二のＬＦＳＲと、前記第二のＬＦＳＲから発生させた２値乱数により前記第一のＬＦＳＲのフィードバック位置を切り替えるセレクタとを備えることを特徴とする請求項１に記載の乱数発生装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、パルス密度変調されたランダムパルス列を生成する装置に用いられる乱数発生装置に関する。

【０００２】

【従来の技術】従来、信号処理装置として、数値を２値パルス列（ここでは、便宜上”１”と”０”の２値で表現されるパルス列とする）の時間当たりの”１”又は”０”のパルスの数、即ちパルス密度で表現して、演算処理を行なうものがある。

【０００３】例えば、図１に示される様に、パルス列で表現された数値の積は、２値パルス列の論理積で求めることができる。１／４のパルス密度を持つパルス列ａと１／２のパルス密度を持つパルス列ｂの論理積をとるパルス列ｃになりそのパルス密度は、１／８となる。精度に注意すれば簡単なデジタル回路で、演算系を構成することが可能である。この場合の演算精度は、パルス列の長さと、”１”の位置の不規則度によって決まることは明かである。

【０００４】このような用途に供される、２値パルス列を得るために一様乱数を発生する乱数源と比較器を用いる方法がある。例えば、基準クロック１２７個分の長さを持つパルス列でパルス密度が、１０／１２７であるようなパルス列を得るためには、１から１２７までの一様乱数を順次発生させ所望の数値１０と比較器で比較し、再生された乱数が１から１０ならば、”１”のパルスを出力し、１１から１２７ならば、”０”のパルスを出力すれば、所望のパルス列を得ることができる。乱数源としては従来、物理雑音を使う方法等が用いられていたが、再現性がない、特性の制御が難しい等の理由により、最近では、簡単なデジタル回路で構成可能であり、良質な２値乱数列を得ることができるＬＦＳＲが良く用いられる。ＬＦＳＲは、例えば図２に示すようにシフトレジスタの一部のビットをフィードバックしてその排他論理和をとって再びシフトインさせるもので、フィードバック位置を注意深く選ぶと、最大周期列信号と呼ばれる２値乱数列が得られる。ｐ段ＬＦＳＲでは最大で”２のｐ乗－１”の周期を持つ２値数列が得られるが、この中で最大の周期を持つものが、最大周期列信号である。

【０００５】例えば、７段のＬＦＳＲで最大周期列信号の得られる回路構成は、図３（ａ）～（ｄ）に示される４種類が存在する。回路の左側に記された式 1～ 4は、特性多項式とよばれ、フィードバック位置を示すものである。図３（ａ）～（ｄ）に示されるＬＦＳＲに最大周期である１２７個のクロックをあたえて発生させた２値乱数列を２値乱数列式（ａ）～（ｄ）に示す。ここでは、１０００００（２進）をＬＦＳＲの初期値として順次シフトアウトされる２値数列を示している。

【０００６】この２値乱数列から、注意深く決めた一定の間隔で取りだして、並列に並べることにより、２進数乱数列を得られる。例えば、前述した１～１２７の乱数列を得るためには、７段のＬＦＳＲのうち最大周期信号を発生するものを用意して、ＬＦＳＲの各ビットを並列に取りだして、７ビットの乱数列とすればよい。これは、最大周期信号列から間隔１で順次７ビット取りだすことに相当する。

【０００７】図３（ａ）～（ｄ）に示されるＬＦＳＲで、シフトイン側のビットをＬＳＢ、シフトアウト側のビットをＭＳＢとし、ＬＦＳＲの初期値を６４（１０進）とすると乱数列式（ａ）～（ｄ）に示す乱数列が得られる。１～１２７の数の出現は、不規則であり前述した一定のパルス密度のランダム２値パルス列の生成に使用することができる。

【０００８】

2

（２値乱数列式）

（ａ）　特殊多項式　$1+X+X^7$　（フィードバック位置；１番目、７番目）　Ｍ系列　1000000111111101010100110011101110100101100011011111011010111001001000111000010111110010101110011010001001111000101000001100000

（ｂ）　特殊多項式　$1+X^6+X^7$（フィードバック位置；６番目、７番目）
M系列　1000000100000110000101000111100100010110011101010011111 0
1000011100010010011011010110111101100011010010111011100 1
100101010111111

（ｃ）　特殊多項式　$1+X^4+X^7$（フィードバック位置；４番目、７番目）
M系列　1000000100010011000101110101101100000110011010100111001 1
1101101000010101011111010010100011011100011111110000111 0
111100101100100

（ｄ）　特殊多項式　$1+X^3+X^7$（フィードバック位置；３番目、７番目）
M系列　1000000100100110100111101110000111111100011101100010100 1
0111110101010000101101111001110010101100110000011011010 1
110100011001000

【０００９】

（乱数列式）

（ａ）　$1+X+X^7$
乱数列　64 1 3 7 15 31 63 127 126 125 122 117 106 85 42 84 41
83 38 76 25 51 103 78 29 59 119 110 93 58 116 105 82
37 75 22 44 88 49 99 70 13 27 55 111 94 61 123 118 109
90 53 107 86 45 91 54 108 89 50 100 73 18 36 72 17 35
71 14 28 56 112 97 66 5 11 23 47 95 62 124 121 114 101
74 21 43 87 46 92 57 115 102 77 26 52 104 81 34 68 9
19 39 79 30 60 120 113 98 69 10 20 40 80 33 67 6 12 24
48 96 65 2 4 8 16 32

（ｂ）　$1+X^6+X^7$
乱数列　64 1 2 4 8 16 32 65 3 6 12 24 48 97 66 5 10 20 40 81 35
71 15 30 60 121 114 100 72 17 34 69 11 22 44 89 51 103
78 29 58 117 106 84 41 83 39 79 31 62 125 122 116 104
80 33 67 7 14 28 56 113 98 68 9 18 36 73 19 38 77 27 54
109 90 53 107 86 45 91 55 111 94 61 123 118 108 88 49
99 70 13 26 52 105 82 37 75 23 46 93 59 119 110 92 57
115 102 76 25 50 101 74 21 42 85 43 87 47 95 63 127 126
124 120 112 96

（ｃ）　$1+X^4+X^7$
乱数列　64 1 2 4 8 17 34 68 9 19 38 76 24 49 98 69 11 23 46 93
58 117 107 86 45 91 54 108 88 48 96 65 3 6 12 25 51 102
77 26 53 106 84 41 83 39 78 28 57 115 103 79 30 61 123
118 109 90 52 104 80 33 66 5 10 21 42 85 43 87 47 95 62
125 122 116 105 82 37 74 20 40 81 35 70 13 27 55 110 92
56 113 99 71 15 31 63 127 126 124 120 112 97 67 7 14 29
59 119 111 94 60 121 114 101 75 22 44 89 50 100 73 18
36 72 16 32

（ｄ）　$1+X^3+X^7$
乱数列　64 1 2 4 9 18 36 73 19 38 77 26 52 105 83 39 79 30 61
123 119 110 92 56 112 97 67 7 15 31 63 127 126 124 120
113 99 71 14 29 59 118 108 88 49 98 69 10 20 41 82 37
75 23 47 95 62 125 122 117 106 85 42 84 40 80 33 66 5

5　　6

11 22 45 91 55 111 94 60 121 115 103 78 28 57 114 101
74 21 43 86 44 89 51 102 76 24 48 96 65 3 6 13 27 54
109 90 53 107 87 46 93 58 116 104 81 35 70 12 25 50
100 72 17 34 68 8 16 32

【００１０】
【発明が解決しようとする課題】しかしながら、このようなＬＦＳＲを使った乱数生成装置を用いて、繰り返しランダム２値パルス列を発生せる場合、ＬＦＳＲの構造が決まれば、パルス列内では、”１”の並びがランダムであるが、繰り返し発生するパルス列どうしを比べると、毎回同じパルス並びとなり、不都合である。
【００１１】本発明は、繰り返し乱数列を発生させる時に、パルス列の並びが異なる乱数列を発生することができる乱数発生装置を提供することを目的とする。
【００１２】また、本発明は、繰り返し乱数列を発生させる時に、毎回ランダムな種類の乱数列を簡単に発生させることができる乱数発生装置を提供することを目的とするものである。
【００１３】
【課題を解決するための手段】この発明による第１の乱数発生装置は、ｎ次の最大周期列信号を生成する第一のＬＦＳＲを備えた乱数発生装置において、上記の目的を達成するため、あらかじめ定められた期間にわたって乱数列を発生した後、前記ＬＦＳＲのフィードバック位置を切り替える手段を設けたことを特徴とする。
【００１４】この発明による第２の乱数発生装置は、上記第１の乱数発生装置において、上記手段が、カウンタと、カウンタの内容に応じてＬＦＳＲのフィードバック位置を切り換えるセレクタとを備えることを特徴とする。
【００１５】この発明による第３の乱数発生装置は、上記第１の乱数発生装置において、上記手段が、ｍビットのシフトレジスタと、該シフトレジスタに格納されたビットデータに従って前記ＬＦＳＲのフィードバック位置を切り替えるセレクタとを備えることを特徴とする。
【００１６】この発明による第４の乱数発生装置は、上記第１の乱数発生装置において、上記手段が、最大周期列信号を生成する第二のＬＦＳＲと、前記第二のＬＦＳＲから発生させた２値乱数により前記第一のＬＦＳＲのフィードバック位置を切り替えるセレクタとを備えることを特徴とする。
【００１７】
【作用】ＬＦＳＲのフィードバック位置を変化させると、繰り返し発生される乱数列のパルスの並びが変化する。
【００１８】なお、ＬＦＳＲを備えた乱数発生装置においてパルスの並びが異なる乱数列を発生させるためには、本発明の方法の他に、ＬＦＳＲの初期値を変更する方法も考えられる。
【００１９】
【実施例】本発明の一実施例に係る乱数発生装置を図面に基づいて具体的に説明すれば、以下の通りである。
【００２０】図４の回路図に示すように、７ビットのシフトレジスタ４０１と、排他的論理和回路４０４と、フィードバック位置を選択するセレクタ４０２とでＬＦＳＲが構成される。
【００２１】このシフトレジスタ４０１の各ビットデータｒ　、ｒ　……ｒ　を並列に取り出し、シフトイン側をＬＳＢシフトアウト側をＭＳＢとした２進数乱数（ｂ０，ｂ１，ｂ２，ｂ３，ｂ４，ｂ５，ｂ６）を得る。
【００２２】さらに、セレクタ４０２には２ビットバイナリカウンタ４０３が接続され、カウンタ４０３はカウントクロック４０７の入力に応じて００→０１→１０→１１→００の順で内容を受け取り、図５の対比図に示すように、”００”に対してはｒ１、”０１”に対してはｒ６、”０１”に対してはｒ４、”１１”に対してはｒ３を選択して、フィードバックするようにしている。
【００２３】例えば、初期値としてカウンタ４０３には”００”を、シフトレジスタ４０１には”００００００１”のデータを設定した場合、フィードバックはｒ１が選択されるので、順次この状態からシフトクロック４０６にクロックを１２７回入れることにより、乱数列式（ａ）に示す乱数列６４、１、３、７、１５、３１、…が得られる。次に、カウントクロック４０７にクロックを少なくとも１回入れる。例えば１回だけ入れるとカウンタ４０３は１つ進み”００”から”０１”に代わり、フィードバックはｒ１からｒ６に切換わる。
【００２４】この状態から再びシフトクロック４０６にクロックを１２７回入れると、今度は乱数列式（ｂ）に示す乱数列６４、１、２、４、８、１６、３２、…が得られ、前回とは異なったものとなる。
【００２５】カウントクロック４０７に入れるクロックはある一定周期毎に少なくとも１回出力する様に制御すればよい、カウント４０３は２ｂｉｔでなくともよくｎビットのうちのｍビットをデコードして、セレクタ４０２を制御してもよい。
【００２６】乱数発生に用いるＬＦＳＲは実施例では７ビットであるが、他のビット数であってもよい。さらに７ビット以外ならば可能なフィードバック位置は、４ケ所以外となるかも知れないのでセレクタ４０２で選択するフィードバック位置と、フィードバック数は実施例以外のものでもよい。
【００２７】このように本実施例では乱数列を繰り返し発生する毎に、図５に示されるように、フィードバック位置をサイクリックに更新し、前回とは異なる種類の乱数列を得ることができる。

【００２８】図６は、本発明の他の実施例に係る乱数発生装置の回路図であり、この装置は７ビットのシフトレジスタ５０１と、排他的論理和回路５０４と、フィードバック位置を切り換えるセレクタ５０２とからなる７ビットの第１ＬＦＳＲ５０５を備える。

【００２９】また、セレクタ５０２には２ビットのシフトレジスタ５０３が接続され、内容に応じてシフトレジスタ５０１のフィードバック位置が切り換わるよう構成されている。シフトレジスタ５０３の内容が”００”ならばｒ11が、”０１”ならばｒ16が、”１０”ならばｒ14が、”１１”ならばｒ13が各々選択される。

【００３０】さらに、シフトレジスタ５０３のシフト入力端子には、第２ＬＦＳＲ５０６のシフトアウト端子が接続され、ＬＦＳＲ５０６のシフトアウトデータをシフトレジスタ５０３に入力できるよう構成されている。ＬＦＳＲ５０６のフィードバック位置はｒ31からのフィードバックに固定されており、２値乱数列式（ａ）に示される最大周期列信号を発生する。

【００３１】シフトレジスタ５０３には初期値として、例えば”１１”が設定される。さらに、シフトレジスタ５０１には、初期値として”００００００１”のデータを設定する。さらにＬＦＳＲ５０６には初期値として、”１０-１１１００”を設定する。シフトレジスタ５０３の内容が”１１”でＬＦＳＲ５０５のフィードバックはｒ13が選択される。順次この状態からシフトクロック５０８にクロックを１２７回入れることにより、２値乱数列として６４、１、２、４、９、１８、３６…が得られる。

【００３２】次にシフトクロック５０９にクロックを少くとも１回入れる。例えば１回だけ入れたとすると、シフトレジスタ５０３の内容は”１１”から”０１”に変わりＬＦＳＲ５０５のフィードバック位置はｒ13からｒ16に切り換わる。この状態から再びシフトクロック５０８にクロックを１２７回入れると、今度は、６４、１、２、４、８、１６、３２…の乱数列が得られ、前回とは異なった乱数列が得られる。以下、乱数列に繰り返し発生することに図７の対比図に示すようにシフトレジスタ５０３の内容が”０１”→”００”→”１０”→…のように変更され、前回とは異なる種類の乱数列が得られることになる。

【００３３】さらに、ＬＦＳＲ５０６で発しされる２値数列は最大周期列信号であり、したがって、シフトレジスタ５０３の内容は繰り返し毎に、毎回ランダムなものとなる。

【００３４】本実施例ではＬＦＳＲ５０５、５０９とも

７段のものにしたが他の段数でも良い。さらにＬＦＳＲ５０６のフィードバック位置は他の位置でもよい。

【００３５】

【発明の効果】この発明の第１の乱数発生装置によれば、ＬＦＳＲのフィードバック位置を切り変えることによりパルスの並びが異なる乱数列を出力させることができる。

【００３６】この発明の第２の乱数発生装置によれば、カウンタの内容を変化させ、カウンタの内容に応じてセレクタでＬＦＳＲのフィードバック位置を切り変えることによりパルスの並びが異なる乱数列を出力させることができる。

【００３７】この発明の第３の乱数発生装置によれば、シフトレジスタのビットデータを変化させることにより、このビットデータの内容に応じてセレクタでＬＦＳＲのフィードバック位置を切り変え、パルスの並びが異なる乱数列を出力させることができる。

【００３８】この発明の第４の乱数発生装置によれば、第２のＬＦＳＲから発生させた２値乱数を変化させることにより、セレクタで第１のＬＦＳＲのフィードバック位置を切り変え、第１のＬＦＳＲからパルスの並びが異なる乱数列を出力させることができる。

【図面の簡単な説明】

【図１】パルス密度方式の演算の原理図である。

【図２】ＬＦＳＲの構成図である。

【図３】フィードバック位置によるＬＦＳＲの出力変化を示す説明図である。

【図４】本発明の構成図である。

【図５】カウンタの内容、フィードバック位置及び特性多項式の対応関係を示す対比図である。

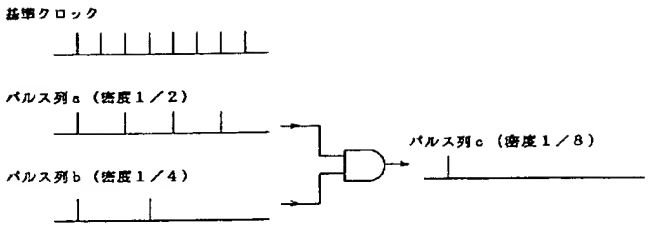
【図６】本発明の構成図である。

【図７】第２ＬＦＳＲの最大周期信号、第２ＬＦＳＲのビットデータ、シフトレジスタの内容及び状態の対応関係を示す対比図である。

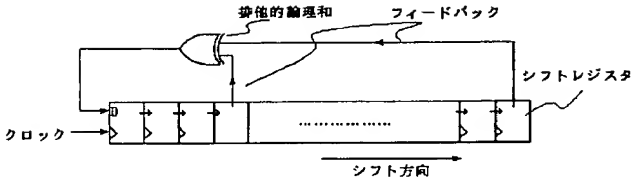
【符号の説明】

４０１　シフトレジスタ
４０２　セレクタ
４０３　カウンタ
４０４　排他的論理和回路
５０１　シフトレジスタ
５０２　セレクタ
５０３　シフトレジスタ
５０４　排他的論理和回路
５０５　第１ＬＦＳＲ
５０６　第２ＬＦＳＲ

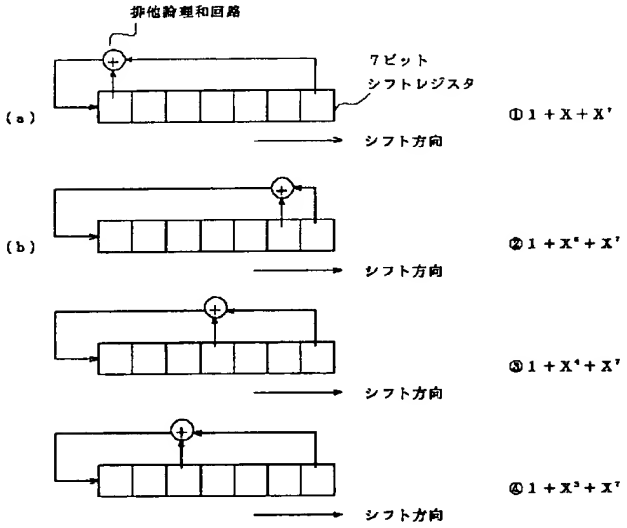
【図１】



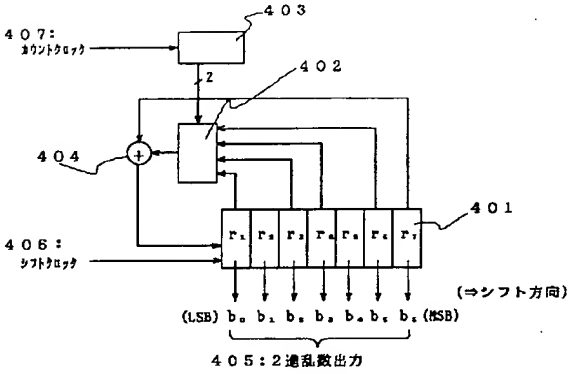
【図２】



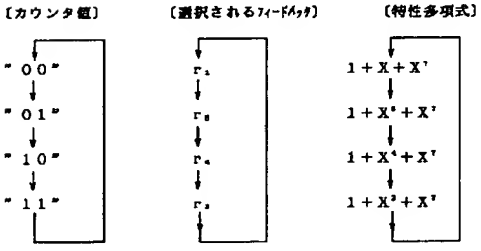
【図３】



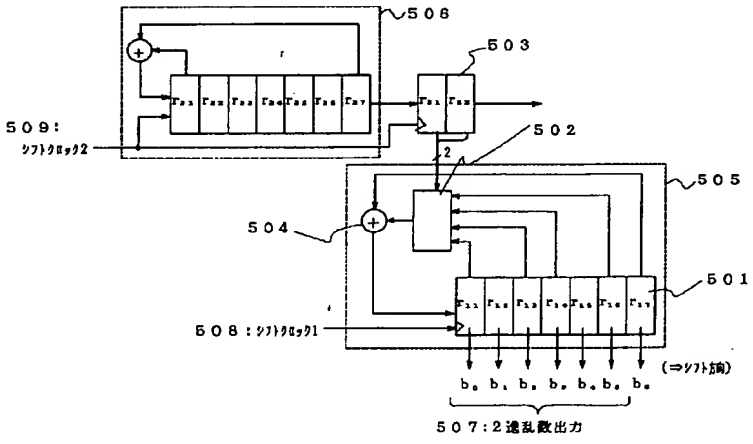
【図４】



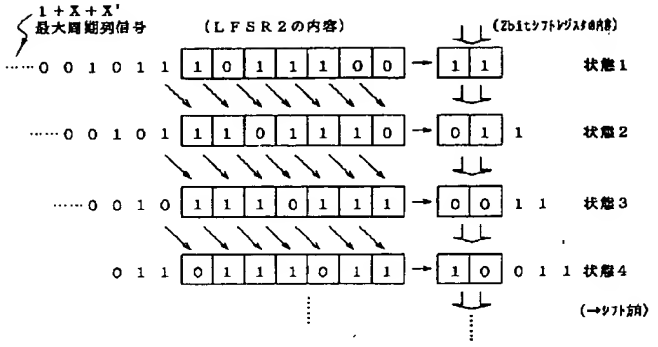
【図５】



【図６】



【図７】


1＋X＋X'
最大周期列信号
（ＬＦＳＲ２の内容）
（2bitシフトレジスタの内容）
……0 0 1 0 1 1
1 0 1 1 1 0 0
1 1
状態１
……0 0 1 0 1
1 1 0 1 1 1 0
0 1 1
状態２
……0 0 1 0
1 1 1 0 1 1 1
0 0 1 1
状態３
0 1 1
0 1 1 1 0 1 1
1 0 0 1 1
状態４
（→シフト方向）